



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,447	10/09/2001	Edward R. Rowe	07844-448001	7875

21876 7590 02/21/2007  
FISH & RICHARDSON P.C.  
P.O. Box 1022  
MINNEAPOLIS, MN 55440-1022

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/21/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/973,447	ROWE, EDWARD R.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 20 November 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-36 and 38 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-16,23-26 and 32-36 is/are rejected.
- 7) ☒ Claim(s) 17-22,27-31 and 38 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date: _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date: _____   | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. This Office action is in response to the RCE filed on 11/20/2006.
2. Claims 1, 2, 4-36 and 38 are pending.

#### ***Continued Examination Under 37 CFR 1.114***

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/20/2006 has been entered.

#### ***Response to Arguments***

4. Applicant's arguments with respect to claims 1, 2, 8-16, 18-31, 34, 35 and 38 have been considered but are moot in view of the new ground(s) of rejection.
5. With respect to applicant's argument that the cited portions of Richards do not overcome the deficiencies of Peinado with respect to claims 4-7, 17, 32, 33 and 36 (Remarks, pg. 11), the new rejections of these claims are based on different cited portions of Richards which anticipates/renders obvious the limitations of these claims as outlined below.

***Claim Rejections - 35 USC § 102***

6. Claims 1, 2, 4-7, 13-15, 32-34 and 36 are rejected under 35 U.S.C. 102(b) as being anticipated by Richards USPN 6,069,957. (hereinafter Richards)

7. As per claim 1, Richards discloses a computer-implemented method for managing access to electronic documents (col. 10:66-12:41), comprising:

- a. associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the encrypted document, the first key being usable to decrypt the encrypted document decryption key; (col. 11:14-22; "CAK")
- b. encrypting the first key to produce an encrypted first key; providing the encrypted first key in a first access controlled manner to users for use in opening the encrypted document; associating with the encrypted first key a second key that can be used to decrypt the encrypted first key; and providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the first key, the second access controlled manner being distinct from the first access controlled manner (11:4-14; 14:21-28; "UEV").

8. As per claim 2, Richards discloses the method further comprising storing the encrypted document decryption key in the encrypted document. Fig. 15. (Code packet

Art Unit: 2132

including the encrypted document decryption key is included with the encrypted content packets)

9. As per claim 4, Richards discloses the method further comprising providing a second encrypted document decryption key for a second encrypted document, the second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the first key is usable to decrypt the second encrypted document decryption key; and associating the first key with the second encrypted document decryption key. Col. 12:8-17; figs. 18 and 19.

10. As per claim 5, Richards discloses the method further comprising providing a third encrypted document decryption key for the second encrypted document, the third encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the third encrypted document decryption key being encrypted so that a third key is usable to decrypt the third encrypted document decryption key; associating the third key with the third encrypted document decryption key; and providing the third key in an access controlled manner to users for use in opening the second document. Fig. 15A, time=10, "CAK," "SK"; Figs. 16-23.

11. As per claim 6, Richards discloses the method further comprising associating a third key with a second encrypted document decryption key for a second document, the

Art Unit: 2132

second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the third key is usable to decrypt the second encrypted document decryption key. Fig. 15A, time=10, "CAK," "SK"; Figs.16-23.

12. As per claim 7, Richards disclose the method further comprises encrypting the third key; associating the second key with the encrypted third key, the second key being usable to decrypt the encrypted third key; and providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the third key. Col. 11:4-16; 14:21-22; 16:4-10.

13. As per claim 13, Richards discloses the method further comprising providing a document decryption key in an access controlled manner to users for opening the encrypted document without using the first key. Col. 6:10-8:29.

14. As per claim 14, Richards discloses the method further comprising associating a unique identifier with the first key. Figure 15. (Encrypted content and key values are submitted via packets comprising header information that uniquely identify the values)

15. As per claim 15, Richards further discloses the unique identifier is stored in the document in association with the encrypted document decryption key to associate the

Art Unit: 2132

first key with the encrypted document decryption key (Code packets are included with the encrypted data packets).

16. As per claims 32-34 and 36, the rejections of claims 1, 2, 4-7 and 13-15 under 35 U.S.C. 102(b) as being anticipated by Richards are incorporated herein. (supra) In addition, a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys. Richards, col. 12:1-37. The aforementioned cover the limitations of claims 32-34 and 36.

***Claim Rejections - 35 USC § 103***

17. Claims 8-12, 23-26 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards in view of Stallings, Cryptography and Network Security, Chapter 6 "Public-Key Cryptography," Chapter 11 "Authentication Applications" and Chapter 12.1 "Pretty Good Privacy" (hereinafter Stallings).

18. As per claims 8-11, the rejection of claim 1 under 33 USC 102(b) as being anticipated by Richards is incorporated herein. Richards does not disclose the step of providing the second key in an access controlled manner comprises sending the second key to users in rights management information specific to systems of the users to whom the second key is sent and sending information used to synthesize the second key in

Art Unit: 2132

rights management information; wherein the rights management information comprises a rights management file; and storing the encrypted first key in rights management file information for the first key. Stallings discloses the use of a certificate to identify characteristics of a key, wherein the certificate includes a subject identifier, period of validity, subject's public-key information, a signature to verify the certificate and key, and extension (pg. 342, figure 11.3); the extensions includes key and policy information, which includes key usage, private-key usage period, certificate policies, policy mappings; the key usage attribute in particular indicates the restrictions imposed as to the purposes for which and the policies under which the certified public key may be used. Pgs. 348-349. As applied to the invention of Richards, a certificate for a key identifies use constraints and characteristics of the key including identification of the key, key usage limitations, a period of validity for the key and ownership of the key. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Richards to include the steps of providing the second key in an access controlled manner comprises sending the second key to users in rights management information specific to systems of the users to whom the second key is sent and sending information used to synthesize the second key in rights management information; wherein the rights management information comprises a rights management file; and storing the encrypted first key in rights management file information for the first key. One would be motivated to do so to ensure the validity of the key in the rights management information, to identify characteristics of the key and



to indicate security policy information for a given key. Pgs. 342, 348, requirement 3.

The aforementioned cover the limitations of claims 8-11.

19. As per claim 12, the rejection of claim 11 under 35 U.S.C. 103(a) as being unpatentable over Richards in view of Stallings is incorporated herein. Richards does not expressly disclose associating a unique identifier with the second key and storing the unique identifier in the rights management information with the encrypted first key. Stallings discloses an overview of PGP wherein one of the salient features of the invention defines an association between an encrypted data decryption key and a key-decrypting key, and between the encrypted data-decrypting key and the encrypted document, to efficiently identify which keys among a collection of keys can decrypt an encrypted document. Pg. 365, Figure 12.3. Moreover, Stallings discloses the use of a key ring to store and organize the keys in a systematic way. Pg. 365, "Key Rings." A key ID is assigned to a key-decrypting key, which identifies a key that decrypts an encrypted data-decryption key. Pg. 365, figure 12.3 and related text. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Richards to include the step of utilizing key identifiers for the purpose of associating key-decrypting keys to an encrypted data-decrypting key, since it is desirable to efficiently associate such decryption keys with their encrypted values. Stallings, pg. 364, 1<sup>st</sup> paragraph. The aforementioned cover the limitations of claim 12.

Art Unit: 2132

20. As per claims 23 and 24, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Richards is incorporated herein. (supra) Richards does not disclose the key to encrypt the document decryption key is a private key and that the first key is a public key. However, it is well known to one of ordinary skill in the art to utilize public key encryption to securely distribute secret keys because public key encryption provides more robust security than symmetric encryption. For example, Stallings discloses a secret key distribution method that ensures confidentiality and authentication wherein a session key is encrypted with a private key and decrypted using a public key. Pgs. 187-189, "Public-Key Distribution of Secret Keys;" in particular, see pgs. 188-189, "Secret Key with Confidentiality and Authentication." As applied to the invention of Richards, private key encryption of the document decryption key ensures that the encrypted digital content comes from a specific trusted source. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Richards so that the encryption key is a private key and the first key is a public key. One would be motivated to so to ensure the origin of the encrypted decryption key and thus ensure the origin of the encrypted document as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 23 and 24.

21. As per claim 25, the rejection of claim 24 under 35 USC 103(a) as being unpatentable over Richards in view of Stallings is incorporated herein. Richards does not disclose providing the first key in an access-controlled manner comprises sending information used to synthesize the first key in a rights management file. Stallings

Art Unit: 2132

discloses the use of a certificate to identify characteristics of a key, wherein the certificate includes a subject identifier, period of validity, subject's public-key information, a signature to verify the certificate and key, and extension (pg. 342, figure 11.3); the extensions includes key and policy information, which includes key usage, private-key usage period, certificate policies, policy mappings; the key usage attribute in particular indicates the restrictions imposed as to the purposes for which and the policies under which the certified public key may be used. Pgs. 348-349. As applied to the invention of Richards, a certification for a key identifies use constraints and characteristics of the key including identification of the key, key usage limitations, a period of validity for the key and ownership of the key. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Richards to include the step of providing the first key in an access-controlled manner comprises sending information used to synthesize the first key in a rights management file. One would be motivated to do so to ensure the validity of the key in the rights management information, to identify characteristics of the key and to indicate security policy information for a given key. Pgs. 342, 348, requirement 3. The aforementioned cover the limitations of claim 25.

22. As per claim 26, Richards discloses a computer-implemented method for accessing an electronic document comprising:

- c. obtaining an encrypted electronic document; obtaining a collection of three or more keys, the keys including keys that are encrypted, the keys and the

document having at least two associations between certain pairs of them, where at least one association is a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where at least one association is a pair consisting of the encrypted second key and an encrypted third key, the association indicating that the decrypted second key can be used to decrypt and thereby make usable the third key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection. Col. 10:66-12:41 (UEV, CAK, CCK, PK, SK, CONTENT).

23. Richards does not disclose expressly defining the associations, such that the associations are used to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access. Stallings discloses an overview of PGP wherein one of the salient features of the invention defines an association between an encrypted data decryption key and a key-decrypting key, and between the encrypted data-decrypting key and the encrypted document, to efficiently identify which keys among a collection of keys can decrypt an encrypted document (pg. 365, figure 12.3). Moreover, Stallings discloses the use of a key ring to store and organize the keys in a systematic way. (pg. 365, "Key Rings") Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Richards such that the key pair and the

Art Unit: 2132

key/document associations expressly defined and to use the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access for a more efficient means of identifying which keys decrypt which document. Stallings, pg. 363, last paragraph-pg. 364, first paragraph. The aforementioned cover the limitations of claim 26.

24. As per claim 35, it is a claim corresponding to claim 26 and it does not teach or define above the information claimed in claim 26. Therefore, claim 35 is rejected as being unpatentable over Richards in view of Stallings for the same reasons set forth in the rejection of claim 26.

25. Claims 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards in view of Stallings, and further in view of Peinado et al. USPN 6,772,340. (hereinafter Peinado)

26. As per claim 16, the rejection of claim 10 under 35 USC 103(a) as being unpatentable over Richards in view of Stallings is incorporated herein. Richards does not disclose wherein the rights management information provides a license and defines a set of permission rights associated with the license. Peinado discloses a digital rights management system wherein digital content is rendered according the rights conferred by the license and specified in the license terms. Col. 3, lines 57-67. As applied to the invention of Richards, downloaded digital content is accessible only if the user has

Art Unit: 2132

proper access rights according to the license terms. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Richards such that the rights management information provides a license and defines a set of permission rights associated with the license. One would be motivated to do so to enforce the rights of the content owner on a user's device. Peinado, 2:44-53. The aforementioned cover the limitations of claim 16.

***Allowable Subject Matter***

27. Claims 17-22, 27-31 and 38 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Communications Inquiry***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jk  
February 17, 2007



Benjamin E. Lanner  
Examiner AU 2132